United States Patent and Trademark Office

Application No.:	09/474,317
Confirmation No.:	2106
Filed:	December 29, 1999
Applicant:	Gregg Homer
Title:	System for Tracking Files Transmitted Over the Internet
Examiner:	Adnan M. Mirza
Art Unit:	2145
Customer No.:	51111
Docket No.:	22292-010100
Client Ref.:	Watermapping

Commissioner for Patents
POB 1450
Alexandria, VA 22313-1450

Revised Appellant's Brief in Support of Appeal Under 37 C.F.R. § 1.191

Dear Commissioner:

This is a revised appeal brief in support of an appeal from the final office action mailed June 16, 2005, rejecting claims 1–27. This revision is in response to the Notification of Noncompliant Appeal Brief mailed July 14, 2006. The following items are included in this brief:

Real Party in Interest

The real party in interest is Gregg Homer, residing at 3329 Coy Drive, Sherman Oaks, California, 91423.

Related Appeals and Interferences

Appellant is not aware of any related appeals or interferences.

Status of Claims

On November 21, 2005, appellant appealed from the final rejection of claims 1–27. A claims appendix of this appeal brief contains a copy of the pending claims.

Status of Amendments

In an after-final amendment filed on September 22, 2005, appellant amended claims 1, 7, 11, 14, 17, 20, and 22. The examiner has entered the amendments to these claims.

Summary of the Claimed Subject Matter

The invention is a method and system of digital file tracking. Page 1, lines 6–8. Digital or other electronic files are tracked as they are sent through a network such as the Internet, Ethernet, or an intranet. Page 2, lines 5–10. Identifying indicia is placed in digital files to identify them. Page 2, lines 11–13. Monitors are placed at particular locations in a network. Page 2, lines 13–15. As a digital file passes through the network, the monitor records whether a digital file with the particular indicia was seen at a location. Page 2, lines 13–19.

With the invention, by tracking where digital files were sent (or received), authors can determine whom to contact in order to secure compensation for use of their works (which are embodied in the digital files). Page 2, lines 19–23. Therefore, this invention will help protect the intellectual property rights of authors including artists, musicians, and other creative professionals. For example, by being able to track where their works were sent or received, authors (such as a songwriter or music artist) may be able to seek royalties for unauthorized playing, exhibition or distribution of their works.

This invention is recited in independent claims 1, 7, 10, 11, 14, 17, 20, 22, and 27 and their dependent claims. Claims 10 and 20 include means-plus-function elements. Some

independent and dependent claims have been grouped for convenience and are summarized below.

Claim 1 provides a method for tracking the transmission of a digital file of interest over the Internet by examining for certain physically associated identifying indicia in the file. Page 4, lines 5–7 and see also figure 1, step 100. These indicia provide encoded information about the file of interest and enable tracking. Packets constituting segments of the file in transit over the Internet are received by an Internet service provider (ISP) or other monitoring entity. Page 5, lines 27–28 and see also figure 1, step 130. A monitor examines the packets' file headers in the packets to determine the presence of specific identifying indicia therein. Page 6, lines 9–12 and see also figure 1, steps 140 and 150. The Internet protocol (IP) header source address for each of the packets containing the specific identifying indicia is recorded. See figure 1, step 160. All received packets are sent unaltered to a next Internet leg in the transmission path of the file. Page 6, lines 21–24 and figure 1, step 135.

Claim 7 provides for a system for tracking an Internet transmission of a digital file containing identifying indicia in a file header. See figure 7a, steps 701–706 and see also page 21, lines 27–29. The system has a server, a router, and a monitor. See figure 2, steps 205, 215, and 210, respectively). Server 205 receives the file. Router 215 routes all packets comprising the file unaltered to a next Internet leg in the transmission path of the file. Page 6, lines 21–24 and figure 1, step 135. In figure 2, monitor 210, which is connected between server 205 and router 215, processes the packets constituting segments of the file. See generally figure 5. Monitor 210 is programmed to: (1) examine file headers in the packets to determine the presence of identifying indicia therein, and (2) record the source Internet address for the file for each of the packets containing the identifying indicia. Page 6, lines 9–12, 21–24; and see also figure 5, step 545.

Claim 10 provides a system for tracking an Internet transmission of a digital file containing identifying indicia in a file header. Page 6, lines 25–28. Referring to figure 2, modem 203 receives the digital file, which is processed by server 205. Monitor 210, connected between modem 203 and server 205, processes packets constituting segments of the file. Monitor 210 is programmed to examine file headers in the packets to determine the presence of the identifying indicia, and to record the source Internet address for the file for each of the packets containing the identifying indicia. Figure 2 illustrates means for sending the received file sends the file unaltered to the next Internet leg in the transmission path of the file. Examples of structure for

this means include router 215 as indicated in figure 2, and as further described on page 6, lines 21–24, of the specification.

Claim 11 provides for a method for tracking the transmission of a digital file over the Internet. See figures 1 and 2. Packets constituting segments of the file in transit over the Internet are received. See figure 1, step 130. The packets' file headers are examined to determine whether there are any identifying indicia. Figure 1, step 150 and figure 5. The source Internet address for those packets containing the identifying indicia are recorded. See figure 5, step 545, and page 24, lines 1–2. All the received packets are sent unaltered to the next Internet leg in the transmission path of the file.

Claim 14 provides for a method for tracking the transmission of a digital file over the Internet. See figures 1 and 2. Identifying indicia is placed in the digital file. See figure 1, step 100. A data communications monitoring device captures all packets of information being transmitted via the Internet without alteration of the captured packets. See figure 1, step 140. Some of the packets are examined to determine the presence of the identifying indicia in the file. See figure 1, step 150. The source and destination Internet addresses are recorded for each of the packets containing the identifying indicia, and the identity of the file associated therewith. See figure 5, step 545, and page 24, lines 1–2.

Claim 17 provides for a method for tracking the transmission of a digital file over the Internet. Packets constituting segments of the file in transit over the Internet are received. The packets are searched for TCP headers containing port numbers indicative of email messages. Page 15, lines 14–19 and see also figure 5, step 510. For those packets that are email messages, a MIME header is searched to discover whether a particular attachment to the email exists. Page 15, lines 22–23 and figure 5, step 520. If an attachment is found, then the header prepended to that file is searched to locate the source Internet address for the file. The source Internet address for the file attached to the email message is recorded. See figure 5, step 545, and page 24, lines 1-2.

Claim 20 provides a system for tracking an Internet transmission of a digital file containing identifying indicia in a file header. See figure 7a, steps 701–706 and see also page 21, lines 27–29. The digital file comprises packets constituting segments of the file. The system has a server, a router, monitoring means, and means for recording. See figure 2, steps 205, 215, and 210, respectively. The server 205 receives the file. The router 215 routes all packets comprising

the file unaltered to a next Internet leg in the transmission path of the file. The monitoring means 210, which are connected between the server 205 and the router 215, examine file headers in the packets to determine the presence of the identifying indicia therein. As disclosed in the specification, such means include the monitoring device 210 illustrated in figure 2, which is a programmable digital processor capable of capturing every packed it receives, and of decoding all layers of the Open Systems Interconnection (OSI) protocol model. Page 6, lines 6–9. Such monitoring means also include a network protocol analyzer, often referred to as a "sniffer," or may be a general-purpose computer, such as a PC, which is programmed to inspect packets received from a server. Page 6, lines 9–12. The means for recording, illustrated in figure 1, step 140, and in figure 5, step 545, records the source Internet address for the file for each of the packets containing the identifying indicia. The recording means may be part of the functionality of the monitoring means previously listed. Page 12, lines 2–3. Structure for this means may also be a file, database, or data storage device. Page 24, lines 1–2.

Claim 22 for the present invention describes a method for tracking the transmission of an MPEG layer 3 (MP3) digital file over the Internet. Page 19, lines 28–31. Packets constituting segments of the file in transit over the Internet are received and searched for an MPEG layer 3 header prepended to the file. See figure 8, step 809 and see also page 20, lines 15–20. The header is searched for identifying indicia. If the identifying indicia are located, then the source Internet address for the file is recorded. See figure 5, step 540 and see also page 24, lines 1–2.

At claim 27, the present invention also provides for a method for tracking the transmission of a digital file over the Internet by a first user to a second user, illustrated in figure 2 as PC 201(a) at user site 201 to PC 225(a) at destination site 225. The second user receives from the first user packets constituting segments of the file in transit over the Internet 220. File headers in the packets are examined to determine the presence of specific identifying indicia therein. The IP header source address is recorded for each of the packets containing the specific identifying indicia. The received packets are sent unaltered to a next Internet leg in the transmission path of the file to the second user. The identifying indicia and the source Internet address are transmitted to a third user.

In the argument section below, appellant grouped the claims into four groups. Group 1 includes the independent claims discussed above. Group 2 includes dependent claims 3, 4, and 18. Claim 3 recites "transmitting said identifying indicia and said source Internet address to a

proprietor of the file." Claim 4 recites "transmitting said identifying indicia and said source Internet address to a remote site." Claim 18 recites "transferring said identifying indicia and said source Internet address to a proprietor of the file." The transmission of the identifying indicia and source Internet address of the file of interest is illustrated in step 160 of figure 1 and described on page 24, lines 2–5.

Group 3 includes dependent claims 5, 8, 12, and 21, which provide for locating the source Internet address in an IP header in various files of interest. Such locating step is shown in step 150 of figure 1, and also in step 540 of figure 5. See also page 23, lines 25–29.

Group 4 includes dependent claims 6, 13, 15, 16, and 23–26. Representative claim 6 recites "said identifying indicia comprises a user-defined character sequence selected from the group consisting of," "an extension to an existing file format, prepended to the file," and "a sequence of bits embedded in the file, and an absence of code in a predefined area within the file." Claims 13, 15, 16, and 23–26 disclose similar limitations. Identifying indicia as referred to by these claims are discussed on page 4, lines 8–14. Figure 1, step 100, illustrates the addition of such indicia to a file.

Grounds of Rejection to Be Reviewed on Appeal

Claims 1–27 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Gabbard (U.S. patent 6,205,432) in view of Eggleston (U.S. patent 6,101,531).

Accordingly, a first grounds of rejection to be reviewed on appeal involves whether claims 1–27 are unpatentable under 35 U.S.C. § 103(a) over Gabbard in view of Eggleston.

Argument

Argument Against First Grounds of Rejection

All claims were rejected under 35 U.S.C. § 103(a) as being unpatentable over Gabbard (U.S. patent 6,205,432) in view of Eggleston (U.S. patent 6,101,531). Appellant believes this rejection is improper for the following reasons.

No Suggestion to Combine Gabbard and Eggleston

There is *no suggestion or motivation to combine* Eggleston with Gabbard. The rejection is based on an improper combination in that neither reference suggests a modification nor an improvement of the system disclosed in the other reference. Eggleston is directed to filtering

transmissions for the purpose of limiting usage of expensive communication paths. Gabbard is directed to a completely different purpose of inserting background references as advertisements. One having ordinary skill in the art would not expect to combine the references.

In fact, Gabbard and Eggleston *teach away* from each other. At column 4, lines 7–8, 12–15, 51–54; column 10, 29–34; abstract, and figure 8, among other locations, Gabbard describes directly or indirectly inserting advertisements in transmitted messages or postings. This is contrary to Eggleston's filtering of transmissions to reduce the usage of costly communications channels as discussed in its abstract, background (column 1), summary (column 2), and elsewhere in Eggleston.

In particular, Eggleston applies filtering to messages so that "only desired data transfers (i.e., those meeting user defined filters) are communicated over the expense-bearing networks between the remote unit and communication server." See Eggleston abstract. This is not compatible with Gabbard's "inserting into an end user communication message a background reference to an advertisement." See Gabbard abstract. While Eggleston is trying to reduce the amount of data transferred, Gabbard does *completely the opposite* action of increasing the amount of data transferred. Based on their intended purposes, this combination of references would be unworkable.

For at least this reason, claims 1–27 should be allowable.

Group 1 (Claims 1, 7, 10, 11, 14, 17, 20, 22, 27)

Claim 1 recites "sending all the received packets unaltered to a next Internet leg in the transmission path of the file."

Claim 7 recites "a router which routes all packets comprising the file unaltered to a next Internet leg in the transmission path of the file."

Claim 10 recites "means for sending the received file unaltered to a next Internet leg in the transmission path of the file."

Claim 11 recites "sending all the received packets unaltered to a next Internet leg in the transmission path of the file."

Claim 14 recites "using a data communications monitoring device to capture all packets of information being transmitted via the Internet without alteration of the captured packets."

Claim 17 recites "sending all the received packets unaltered to a next Internet leg in the transmission path of the file."

Claim 20 recites "a router for routing all packets comprising the file unaltered to a next Internet leg in the transmission path of the file."

Claim 22 recites "sending all the received packets unaltered to a next Internet leg in the transmission path of the file."

Claim 27 recites "sending the received packets unaltered to a next Internet leg in the transmission path of the file to the second user."

The combination of Gabbard and Eggleston do not show or suggest each and every recited feature of the present invention. In particular, the references do not show or suggest the recited limitations of the claims in this group.

Combination of Gabbard and Eggleston Falls Short of Claimed Invention

Even if Gabbard were combined with Eggleston, and there is no suggestion to do this for the reasons stated above, the *combination would still fall short* of the invention as recited in the claims. The combination of Gabbard and Eggleston would be a system or technique that inserts advertisements into messages and also filters messages at the same time. The filtering may be based on user-defined filters. The messages which pass through the filter would include the inserted advertisements.

During operation, some messages may not pass through because of the filtering, but a message passing through would have additional data (i.e., an inserted advertisement). The message passing through or being transmitted is *altered* compared to the original message.

Furthermore, according to the system, some messages may be *additionally altered*. At column 12, lines 7–17, Gabbard describes searching a message for the text "MIME-Version" in a header field. If the message is not in a MIME format, it is checked for attachments included within the text of the message converted into a MIME format. Messages that are not in the MIME format are converted. In addition to having an advertisement inserted, a message may be *further altered* if it is changed to a MIME format, which is *different format* from the original message.

Gabbard describes that regardless of whether the message is converted, a background reference is always inserted and thus always *altered*. See, for example, column 12, lines 31–32 which states, "Next, a MIME multipart/alternative part with HTML is added in step 510." Column 12, lines 47–48 states "a background reference insertion process is executed in step 512." See figure 4, step 312 ("Background Reference Insertion Process"); figure 5, step 418

("Insert Background Reference"); and figure 10, step 510 ("Add a Multipart/Alternative Part"), step 512 ("Background Reference Insertion Process"). Column 11, lines 34–37 states "subsequently, as discussed above with respect to background reference insertion process 312, a background reference is inserted into the message."

As has been stated, a message passing through the Gabbard and Eggleston system would be altered by an inserted advertisement. Further still, Eggleston describes *altering* some messages. See, for example, column 3, lines 21–31, which states, "A select and summary listing or index is used to provide user flexibility in reviewing and requesting otherwise filtered data. . . . As new data is reviewed and filtered for transfer, identifying/summary information is captured for any non-qualifying data." Further, "messages passing all criteria but message size could still be received in a truncated size meeting the message size criterion." Truncating a message removes a portion of the original message before transmitting it. Thus, even when considered individually, Eggleston describes *altering* some messages from their original form.

Therefore, *Gabbard and Eggleston, considered individually or in combination, do not show or suggest transmitting messages unaltered.* For at least this reason, claims 1, 7, 10, 11, 14, 17, 20, 22, and 27 should be allowable. Claims 2–6, 8–9, 12–13, 15–16, 18–19, 21, and 23–26 are dependent claims based on these claims are should be allowable for at least the similar reasons as discussed for the claims in this group.

Some of the claims in this group include limitations discussed in other groups. These claims should be allowable for at least similar reasons as discussed in this group and for the additional reasons discussed in other groups.

Group 2 (Claims 3, 4, 18)

Claim 3 recites "transmitting said identifying indicia and said source Internet address to a proprietor of the file."

Claim 4 recites "transmitting said identifying indicia and said source Internet address to a remote site."

Claim 18 recites "transferring said identifying indicia and said source Internet address to a proprietor of the file."

The references do not show or suggest the recited limitations of the claims in this group. Gabbard and Eggleston do not teach or suggest "transmitting said identifying indicia and said

source Internet address." More specifically, Eggleston describes a predetermined number of user-definable filter attributes. In particular, column 8, lines 45–50 describes:

> messages passing all criteria but message size could still be received in a truncated size meeting the message size criterion. Alternatively, messages failing the author or subject filters could still be passed with header information, by setting all rejected message to be passed with a text truncation size of "0" bytes.

No identifying indicia or a source Internet address is transmitted in Eggleston. Clients in Eggleston only receive filtered information based on user defined filter attributes.

For at least this reason, the claims in this group should be allowable. Claim 19 is dependent on claim 18 and should be allowable for at least a similar reason as discussed for these claims.

Some of the claims in this group incorporate limitations of claims in other groups. These claims should be allowable for at least similar reasons as discussed in the other groups and for the additional reason discussed in this group.

Group 3 (Claims 5, 8, 12, 21)

Claim 5 recites "locating the source Internet address in an IP header for the file containing the attachment."

Claim 8 recites "locate the source Internet address in an IP header for the file containing the attachment."

Claim 12 recites "locating the source Internet address in an IP header for the file containing the attachment, when said identifying indicia is found."

Claim 21 recites "locating the source Internet address in an IP header for the file containing the attachment."

The references do not show or suggest the recited limitations of the claims in this group. Gabbard and Eggleston do not teach or suggest "locating the source Internet address in an IP header" for the file containing the attachment.

As has been discussed, Eggleston describes determining whether a message is in a conventional MIME format by searching for the message "MIME-Version" in a header field. If it is not in a MIME format, the message is converted into a MIME format. Eggleston does not teach or describe locating the source Internet address in an IP header for the file containing the attachment.

For this reason, the claims in this group should be allowable.

Some of the dependent claims in this group incorporate limitations of claims in other groups. These claims should be allowable for at least similar reasons as discussed in the other groups and for the additional reason discussed in this group.

Group 4 (Claims 6, 13, 15, 16, 23–26)

Representative claim 6 recites "said identifying indicia comprises a user-defined character sequence selected from the group consisting of," "an extension to an existing file format, prepended to the file," and "a sequence of bits embedded in the file, and an absence of code in a predefined area within the file."

See claims 13, 15, 16, and 23–26 for limitations.

The references do not show or suggest the recited limitations of the claims in this group. At column 16, lines 32–33, Gabbard describes an email message receiving steps including an external e-mail server program to determine when a new email message is available. Gabbard clearly does not teach or suggest the recited invention.

For this reason, the claims in this group should be allowable.

Some of the dependent claims in this group incorporate limitations of claims in other groups. These claims should be allowable for at least similar reasons as discussed in the other groups and for the additional reason discussed in this group.

Conclusion

For the above reasons, appellant submits that the examiner's rejections of the claims should be withdrawn, and reversal of the decision is respectfully requested.

Respectfully submitted,

Aka Chan LLP

/Melvin D. Chan/

Melvin D. Chan
Reg. No. 39,626

Attachments: Claims Appendix
Evidence Appendix

Aka Chan LLP
900 Lafayette Street, Suite 710
Santa Clara, CA 95050
Tel: (408) 701-0035
Fax: (408) 608-1599
E-mail: mcl@akachanlaw.com

Claims Appendix

1. A method for tracking the transmission of a digital file over the Internet comprising the steps of:

receiving packets constituting segments of the file in transit over the Internet;

examining file headers in said packets to determine the presence of specific identifying indicia therein;

recording the Internet Protocol header source address for each of the packets containing said specific identifying indicia; and

sending all the received packets unaltered to a next Internet leg in the transmission path of the file.

2. The method of claim 1, including the additional step of recording the Internet Protocol header destination address for the file.

3. The method of claim 1, including the additional step of transmitting said identifying indicia and said source Internet address to a proprietor of the file.

4. The method of claim 1, including the additional step of transmitting said identifying indicia and said source Internet address to a remote site.

5. The method of claim 1, wherein said examining step further includes:

searching said file headers for TCP headers containing port numbers indicative of an email message;

searching each of said packets, in which port numbers indicative of email messages were found, for an attachment; and

when said attachment is found, locating the source Internet address in an IP header for the file containing the attachment.

6. The method of claim 1, wherein said identifying indicia comprises a user-defined character sequence selected from the group consisting of:

an extension to an existing file format, prepended to the file;

a sequence of bits embedded in the file; and

an absence of code in a predefined area within the file.

7. A system for tracking an Internet transmission of a digital file containing identifying indicia in a file header, the system comprising:

a server which receives the file;

a router which routes all packets comprising the file unaltered to a next Internet leg in the transmission path of the file; and

a monitor, connected between said server and said router, which processes packets constituting segments of the file;

wherein said monitor is programmed to:

examine file headers in said packets to determine the presence of said identifying indicia therein; and

record the source Internet address for said file for each of the packets containing said identifying indicia.

8. The system of claim 7, wherein said monitor is further programmed to:

search said file headers for TCP headers containing port numbers indicative of email messages;

search each of said packets, in which port numbers indicative of email messages were found, for an attachment; and

locate the source Internet address in an IP header for the file containing the attachment.

9. The system of claim 7, wherein said identifying indicia comprises a user-defined character sequence selected from the group consisting of:

an extension to an existing file format, prepended to the file;

a sequence of bits embedded in the file; and

an absence of code in a predefined area within the file.

10. A system for tracking an Internet transmission of a digital file containing identifying indicia in a file header, the system comprising:

a modem which receives the file;

a server for processing the file;

a monitor, connected between said modem and said server, which processes packets constituting segments of the file; wherein said monitor is programmed to:

examine file headers in said packets to determine the presence of said identifying indicia therein; and

record the source Internet address for said file for each of the packets containing said identifying indicia; and

means for sending the received file unaltered to a next Internet leg in the transmission path of the file.

11. A method for tracking the transmission of a digital file over the Internet comprising the steps of:

receiving packets constituting segments of the file in transit over the Internet;

examining file headers in said packets to determine the presence of specific identifying indicia therein;

recording, for each of the packets containing said identifying indicia, the source Internet address for the file; and

sending all the received packets unaltered to a next Internet leg in the transmission path of the file.

12. The method of claim 11, wherein said examining step further includes:

searching said file headers for TCP headers containing port numbers indicative of email messages;

searching each of said packets, in which port numbers indicative of email messages were found, for a MIME header indicative of an attachment; and

when said MIME header indicative of an attachment is found:

searching a header directly prepended to the file to find said identifying indicia therein, when said MIME header is indicative of an attachment containing a type of said file sought: and

locating the source Internet address in an IP header for the file containing the attachment, when said identifying indicia is found.

13. The method of claim 11, wherein said identifying indicia comprises a user-defined character sequence selected from the group consisting of:

an extension to an existing file format, prepended to the file; a sequence of bits embedded in the file; and

an absence of code in a predefined area within the file.

14. A method for tracking the transmission of a digital file over the Internet comprising the steps of:

placing identifying indicia in said digital file;

using a data communications monitoring device to capture all packets of information being transmitted via the Internet without alteration of the captured packets;

examining certain ones of said packets to determine the presence of said identifying indicia in said file; and

recording the source and destination Internet addresses for each of the packets containing said identifying indicia, and the identity of the file associated therewith.

15. The method of claim 14, wherein said identifying indicia is prepended to said header.

16. The method of claim 14, wherein said identifying indicia is embedded in said file.

17. A method for tracking the transmission of a digital file over the Internet comprising the steps of:

receiving packets constituting segments of the file in transit over the Internet; searching said packets for TCP headers containing port numbers indicative of email messages;

searching each of said packets, in which said port numbers indicative of email messages were found, for a MIME header indicative of an attachment;

when said MIME header indicative of an attachment is found:

searching a header directly prepended to the file to locate an identifying indicia therein, when said MIME header is indicative of an attachment containing a type of said file sought;

locating a source Internet address in an IP header for the file containing the attachment containing the type of said file sought, when said identifying indicia is located; and

recording, for each of the packets containing said identifying indicia, the source Internet address for the file; and

sending all the received packets unaltered to a next Internet leg in the transmission path of the file.

18. The method of claim 17, including the additional step of transferring said identifying indicia and said source Internet address to a proprietor of the file.

19. The method of claim 18, including the additional step of transferring additional information in said file to the proprietor of the file.

20. A system for tracking an Internet transmission of a digital file containing identifying indicia in a file header, wherein said file comprises a plurality of packets constituting segments of the file, the system comprising:

a server for receiving the file;

a router for routing all packets comprising the file unaltered to a next Internet leg in the transmission path of the file;

monitoring means, connected between said server and said router, for examining file headers in said packets to determine the presence of said identifying indicia therein; and

means for recording the source Internet address for said file for each of the packets containing said identifying indicia.

21. The system of claim 20, wherein said monitoring means further comprises searching means for:

locating said file headers for TCP headers containing port numbers indicative of email messages;

locating each of said packets, in which port numbers indicative of email messages were found, for an attachment; and

locating the source Internet address in an IP header for the file containing the attachment.

22. A method for tracking the transmission of a digital file over the Internet comprising the steps of:

receiving packets constituting segments of the file in transit over the Internet;

searching said packets for an MPEG Layer 3 header prepended to the file;

searching said MPEG Layer 3 header for identifying indicia located therein, if said MPEG Layer 3 header is located;

locating the source Internet address in an IP header for the file containing said identifying indicia, if said identifying indicia is located;

recording, for each of the packets containing said identifying indicia, the source Internet address for the file; and

sending all the received packets unaltered to a next Internet leg in the transmission path of the file.

23. The method of claim 22, wherein said identifying indicia is located in a header having a field indicating that the frame size thereof is zero bytes in length.

24. The method of claim 22, wherein said identifying indicia is located in a header having a frame size field indicating that there is no information field appended to the frame size field.

25. The method of claim 22, wherein said identifying indicia comprises a user-defined character sequence located in the 'frame ID' and 'flags' fields of an ID3v2 frame header.

26. The method of claim 22, wherein said identifying indicia comprises a user-defined character sequence selected from the group consisting of:

an extension to an existing file format, prepended to the file;

a sequence of bits embedded in the file; and

an absence of code in a predefined area within the file.

27. A method for tracking the transmission of a digital file over the Internet by a first user to a second user comprising the steps of:

receiving from the first user packets constituting segments of the file in transit over the Internet;

examining file headers in said packets to determine the presence of specific identifying indicia therein;

recording the Internet Protocol header source address for each of the packets containing said specific identifying indicia;

sending the received packets unaltered to a next Internet leg in the transmission path of the file to the second user; and

transmitting said identifying indicia and said source Internet address to a third user.

Evidence Appendix

None

Related Proceedings Appendix

None